

October 10, 2016

Via Electronic Filing

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street SW
Washington, DC 20554

**Ex Parte: Protecting the Privacy of Customers of Broadband and Other
Telecommunications Services, WC Docket No. 16-106**

Dear Secretary Dortch:

The American Association of Advertising Agencies (“4A’s”), American Advertising Federation (“AAF”), Association of National Advertisers (“ANA”), Direct Marketing Association (“DMA”), Interactive Advertising Bureau (“IAB”), and Network Advertising Initiative (“NAI”) provide these comments to the Federal Communications Commission (“Commission” or “FCC”) on its proceeding related to the privacy of telecommunications customers.¹ We are the leading trade associations for advertising and marketing industries, collectively representing more than 5,000 U.S. corporations across the full spectrum of businesses that participate in and shape today’s media landscape.

We write to express our deep concern regarding a proposed last-minute change to privacy rules for Broadband Internet Access Services (“BIAS”), which would significantly harm online commerce. Chairman Tom Wheeler has released a fact sheet stating that the Commission is considering a proposed rule that would require opt-in consent to use and share “sensitive data,” a term that the Commission would expand to include web browsing and application use history when linked to a device alone. This would be an unprecedented step. As explained below, this proposal would upend the established and thriving Internet economy, which relies on the support of data-driven advertising.

This counterproductive proposal has been introduced late in the Commission’s process, with little opportunity for public review and comment. The fact sheet offers no explanation for this proposed departure from the accepted industry practice and customer expectation that the collection and use of web viewing and application use data for advertising purposes is subject to an opt-out choice. There is no record of consumer harm to justify treating web viewing and application use history as sensitive or for it to be subject to opt-in consent. The current opt-out approach has helped fuel the successful commercial Internet, made the U.S. the global Internet leader, and continues to deliver extraordinary products and services to consumers. We believe that mandating an opt-in requirement in these areas would seriously inhibit the ability of BIAS to succeed in the developing marketplace. We also believe industry’s self-regulatory programs for

¹ Filed pursuant to 47 C.F.R. § 1.1206.

web viewing and application use data are the most appropriate and effective framework for protecting consumer privacy while ensuring the Internet remains a platform for innovation and continued economic development.

I. There has not been sufficient time for the public or the Commission to consider this proposal.

We submit that this proposal merits substantial additional procedural protections. To date, the only public notice of the proposal has come from media reports and from a blog post and fact sheet published by Chairman Wheeler. It was not included in the Commission's earlier proposed Order that was released for comment, and the Commission has not released the text of the new approach for public review and comment. This process is insufficient in light of the significant impact and unprecedented nature of the proposed approach to regulating online data. The Commission should afford industry and the public a meaningful opportunity to provide information to inform the Commission's decision. By not offering this opportunity, the Commission shortchanges the administrative process and undermines the legitimacy of any resulting decision.

II. The data-driven and ad-supported economy benefits consumers and fuels economic growth.

Data-driven online commerce and advertising drive Internet growth and deliver innovative tools and services embraced by consumers and businesses. The current online ecosystem subsidizes content and programming that consumers value, promotes innovation, and grows the economy.² The continued health of this ecosystem depends on access to data. A recent study commissioned by DMA's Data-Driven Marketing Institute ("DDMI") and conducted independently by Harvard Business School Professor John Deighton and recent Columbia University Adjunct Professor Peter Johnson, entitled *The Value of Data: Consequences for Insight, Innovation, & Efficiency in the U.S. Economy* ("Value of Data"), quantifies the concrete economic benefits of data.³ The *Value of Data* study found that the Data-Driven Market Economy ("DDME") generates vital revenue and jobs for the U.S. economy. Specifically, the study found that the use of data-driven marketing added \$202 billion in revenue to the U.S. economy and fueled more than 966,000 jobs in 2014.⁴ The study also found that the

² A recent Zogby Analytics poll commissioned by the Digital Advertising Alliance ("DAA") shows that consumers assign a value of almost \$1,200 a year to ad-supported online content. DAA, *Zogby Poll: Americans Say Free, Ad-Supported Online Services Worth \$1,200/Year; 85% Prefer Ad-Supported Internet to Paid*, PR Newswire (May 11, 2016 8:30 AM), <http://www.prnewswire.com/news-releases/zogby-poll--americans-say-free-ad-supported-online-services-worth-1200year-85-prefer-ad-supported-internet-to-paid-300266602.html>.

³ Deighton and Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* (2015) (hereinafter "*The Value of Data*").

⁴ *Id.* at 19.

U.S. DDME provides the American people with high-value jobs.⁵ The undersigned associations are committed to responsible data practices, and are concerned that the unprecedented restrictions now being proposed could threaten these economic benefits and consumers' access to the products and services they have come to expect.

III. Web browsing and application use data is not sensitive data, and requiring opt-in consent for such data would stifle e-commerce and bombard consumers with unnecessary notices.

The FCC's sister agency, the Federal Trade Commission ("FTC"), has long held that "sensitive data" encompasses a limited set of data types and does not include web browsing or application use data. In its comments to the FCC regarding this proposed Order, the FTC listed data types it considers as sensitive, "e.g., Social Security numbers and children's, financial, health, and geolocation data."⁶ The FTC's 2012 Privacy Report, based on public comments on this issue, agreed that "information about children, financial and health information, Social Security numbers, and precise geolocation data...are sensitive" and that companies should obtain consent from consumers before collecting such data.⁷ Web browsing and application use data are notably absent from this list, although the collection and use of such data for advertising was already commonplace at the time.

In contrast, in the 2012 report, the FTC endorsed the approach of offering an opt-out choice for the use of web browsing data for advertising.⁸ This approach built on the FTC's earlier staff report in 2009 discussing the collection and use of data for online behavioral advertising ("OBA").⁹ In the 2009 report, the FTC made a distinction between sensitive data (*i.e.*, "data about children, health, or finances") and non-sensitive data.¹⁰ The FTC recommended that companies obtain affirmative express consent for the use of a limited category of sensitive data (*e.g.*, financial data, health data, data about children, precise geolocation, and Social Security numbers) for OBA, but provide notice and choice for the collection and use of other non-sensitive data for OBA.¹¹ Far from agreeing with the FTC's existing framework, the

⁵ *Id.*

⁶ FTC, *Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission*, 21 (May 27, 2016) https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-federal-trade-commission-federal-communications-commission/160527fcccomment.pdf.

⁷ FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers*, 58-59 (Mar. 2012) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

⁸ *Id.* at 52-54.

⁹ FTC, *Self-Regulatory Principles for Online Behavioral Advertising: Behavioral Advertising Tracking, Targeting, & Technology* (Feb. 2009) <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf>.

¹⁰ *Id.* at 12.

¹¹ *Id.* at 11-12.

proposal before the Commission would expand the category of “sensitive data” far beyond what the FTC has ever recognized.

The new proposal also departs from judicial rulings on web browsing data. Numerous courts have considered challenges to the collection and use of web browsing data for advertising through multiple techniques. Repeatedly, courts considering such practices have found that the advertising use of web browsing histories tied to device information does not harm or injure consumers.¹² These cases support the view that web browsing data, and analogous data collected on application usage, are not sensitive for consumers.

By categorizing web browsing and application use data as “sensitive,” the current proposal would require BIAS providers to obtain opt-in consent for the use and sharing of such data, including for advertising. This would be a radical departure from current industry practice, the longstanding views of the FTC, and case law that support the provision of an opt-out choice for the collection and use of web browsing data and application use data. Consistent with this settled consensus, we believe that opt-out choice continues to provide the right balance because it enables consumers to exercise control over online data, while allowing beneficial and responsible data use to continue. The change proposed by the Commission to expand the definition of sensitive data is likely to chill innovation and frustrate consumers as this will likely result in consumers facing a bombardment of disruptive opt-in notices.

IV. Industry self-regulation is the appropriate and proven approach to foster innovation and provide consumers with choice.

More than seven years ago, industry responded to the FTC’s calls for notice and choice with respect to the collection and use of online data, and delivered a robust, enforceable set of self-regulatory principles implemented through the Digital Advertising Alliance (“DAA”).¹³ These principles already address both web browsing and application use data. The DAA’s self-regulatory approach aligns with the FTC’s approach to non-sensitive data and provides a flexible and innovative approach that has kept pace with an ever-changing marketplace. The DAA framework is vigorously enforced by industry watchdogs that respond to consumer complaints and actively monitor compliance.¹⁴ The rapid growth of the DAA program shows why self-

¹² See, e.g., *Mount v. PulsePoint, Inc.*, No. 13 Civ. 6592 (NRB), at *34-35 (S.D.N.Y. Aug. 17, 2016); *LaCourt, et al. v. Specific Media, Inc.*, SAVC 10-1256-GW(JCGx), at *8 (C.D. Cal. Apr. 28, 2011), <http://www.scribd.com/doc/54537062/La-Court-v-Specific-Media-Granting-Dismissal-Motion>.

¹³ DAA, *Self-Regulatory Principles* (2009-2015) <http://aboutads.info/principles>; NAI, *Code of Conduct* (2015) http://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf. NAI was founded more than 15 years ago to create robust self-regulation in the industry, and the DAA’s program has built on the NAI program by expanding the reach of self-regulation to the entire digital advertising industry.

¹⁴ If a company fails to meet its obligations under the Program, the DAA’s independent accountability programs, run by the Council for Better Business Bureaus (“CBBB”) and the DMA, will work to bring a company into

regulation is best suited to provide the flexibility to accommodate new technologies, while protecting consumer privacy.

The DAA's successful approach drew praise at a February 2012 event at the White House where the then-Chairman of the FTC, the then-Secretary of Commerce, and White House and White House officials publicly praised the DAA's cross-industry initiative. The White House recognized the DAA as "an example of the value of industry leadership as a critical part of privacy protection going forward."¹⁵ The DAA's ongoing work in expanding its principles has garnered additional praise, including from FTC Commissioner Ohlhausen, who has stated that the DAA "is one of the great success stories in the [privacy] space."¹⁶ The proposal now before the Commission would upend this successful program in relation to BIAS providers, and stifle innovation in the process. We urge the Commission to reconsider this proposal or, at a minimum, to take the time to review it through the regular notice and comment process. After due consideration, the Commission should instead adopt the DAA's time-tested approach to online data collection and use, which is endorsed by the FTC and the White House.

* * *

We appreciate the opportunity to submit these comments, and we look forward to working with the FCC on this important issue.

Respectfully submitted,

American Advertising Federation
American Association of Advertising Agencies
Association of National Advertisers
Direct Marketing Association
Interactive Advertising Bureau
Network Advertising Initiative

CC: Stuart Ingis, Venable LLP
Michael Signorelli, Venable LLP

compliance. The programs may refer unresolved matters to the FTC. The CBBB publicly reports its decisions and has brought more than 60 enforcement actions since the DAA Principles went into effect.

¹⁵ Speech by Danny Weitzner, *We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age* (February 23, 2012), <http://www.whitehouse.gov/blog/2012/02/23/we-can-t-waitobama-administration-calls-consumer-privacy-bill-rights-digital-age>.

¹⁶ Katy Bachman, *FTC's Ohlhausen Favors Privacy Self-Regulation*, Adweek (June 3, 2013, 2:50 PM), <http://www.adweek.com/news/technology/ftcs-ohlhausen-favors-privacy-self-regulation-150036>.